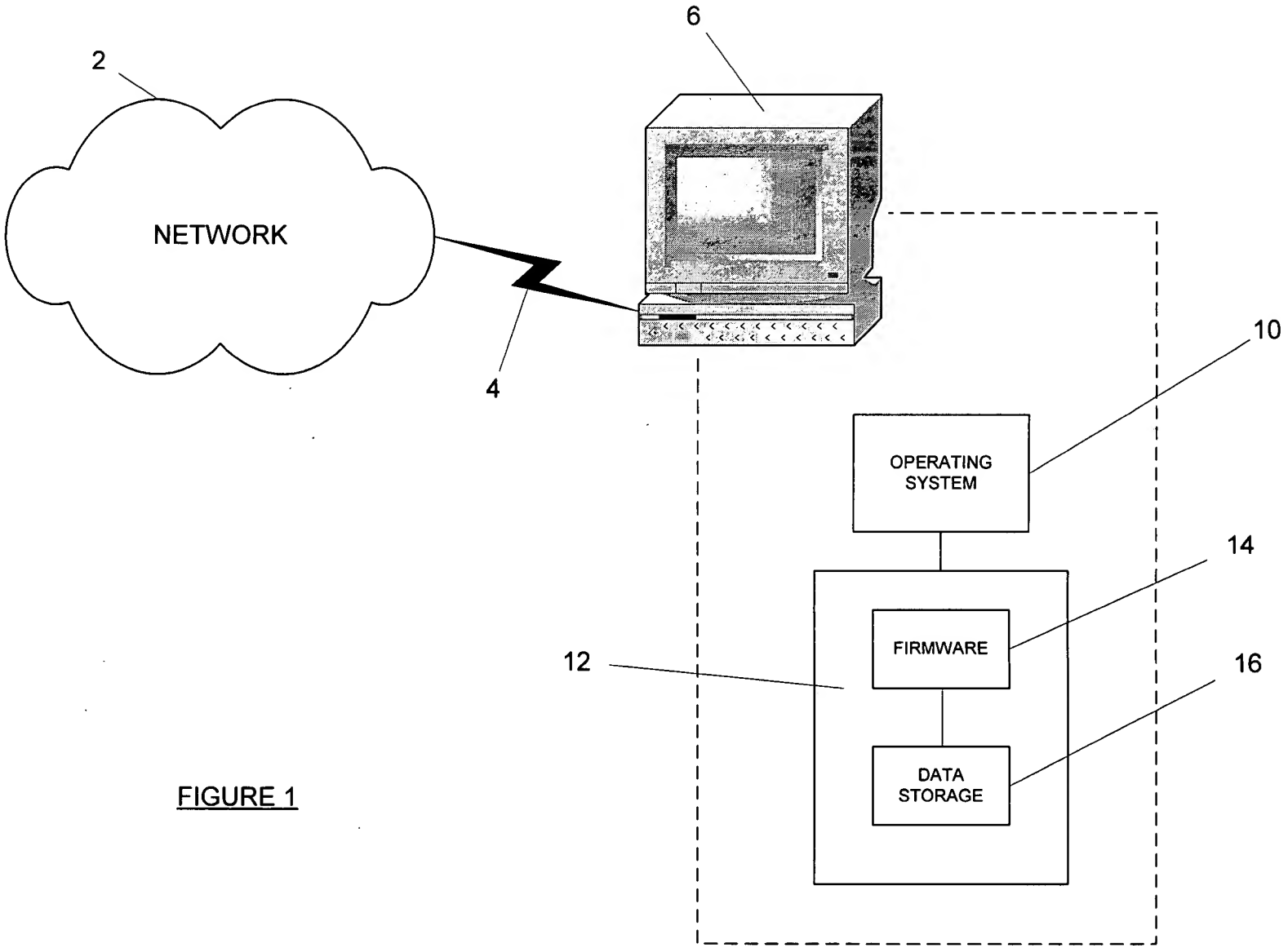
6
2
NETWORK
4
10
OPERATING SYSTEM
14
12
FIRMWARE
16
DATA STORAGE

FIGURE 1

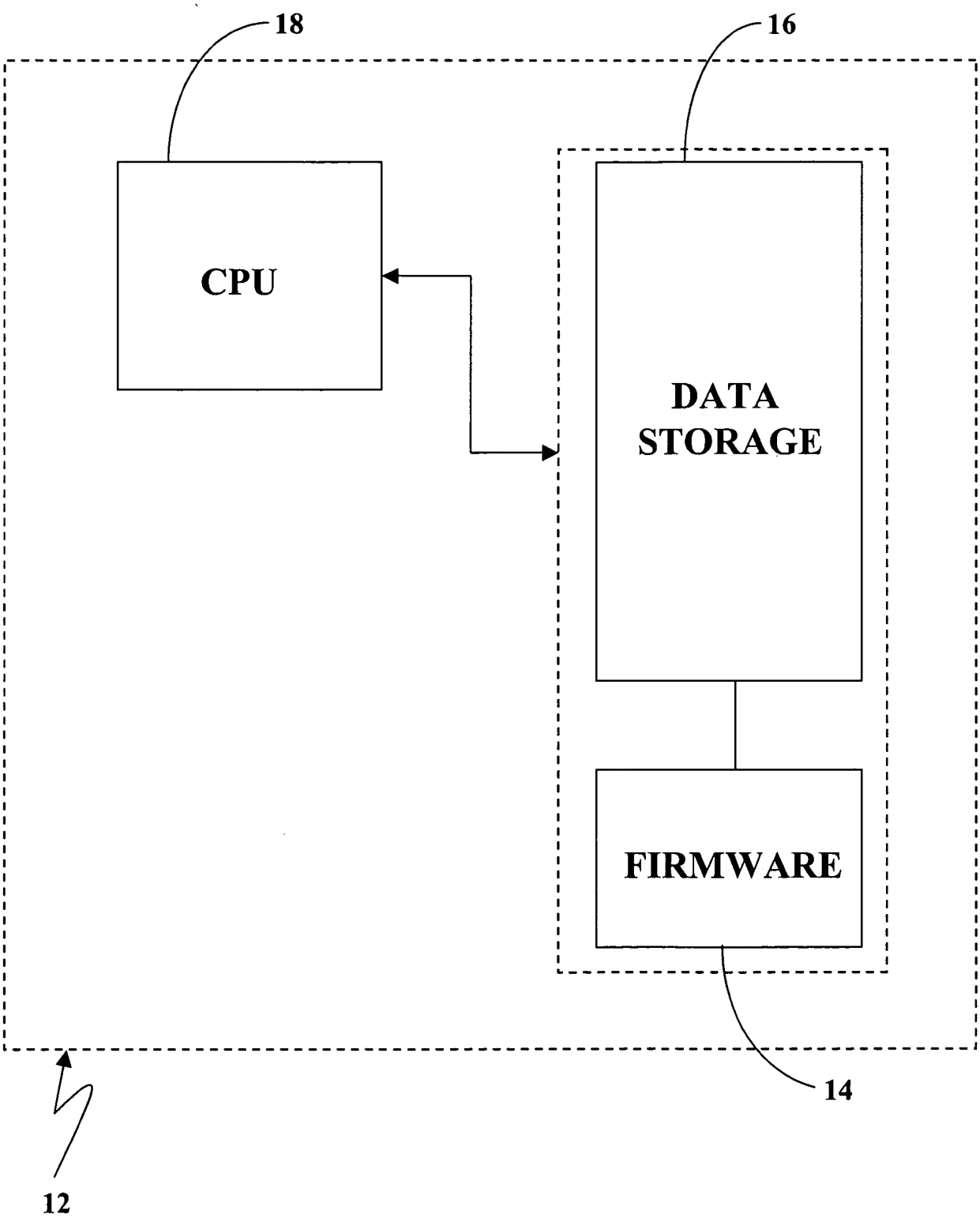

FIG. 2

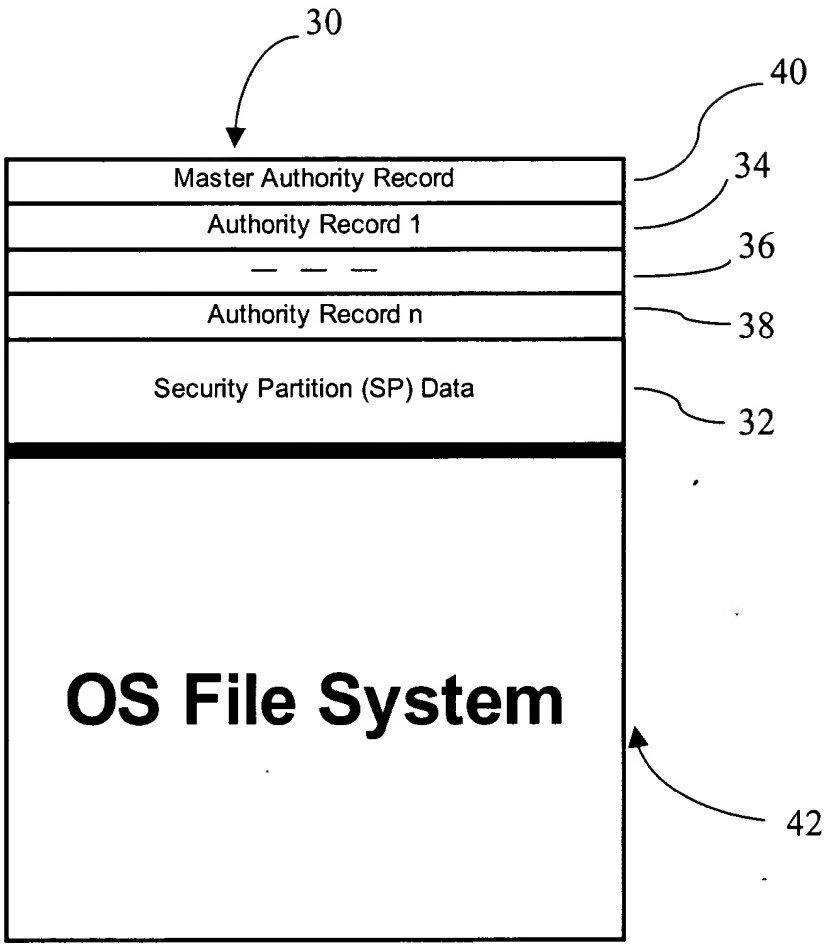
30
40
Master Authority Record
34
Authority Record 1
36
— — —
Authority Record n
38
Security Partition (SP) Data
32
OS File System
42

FIG. 3

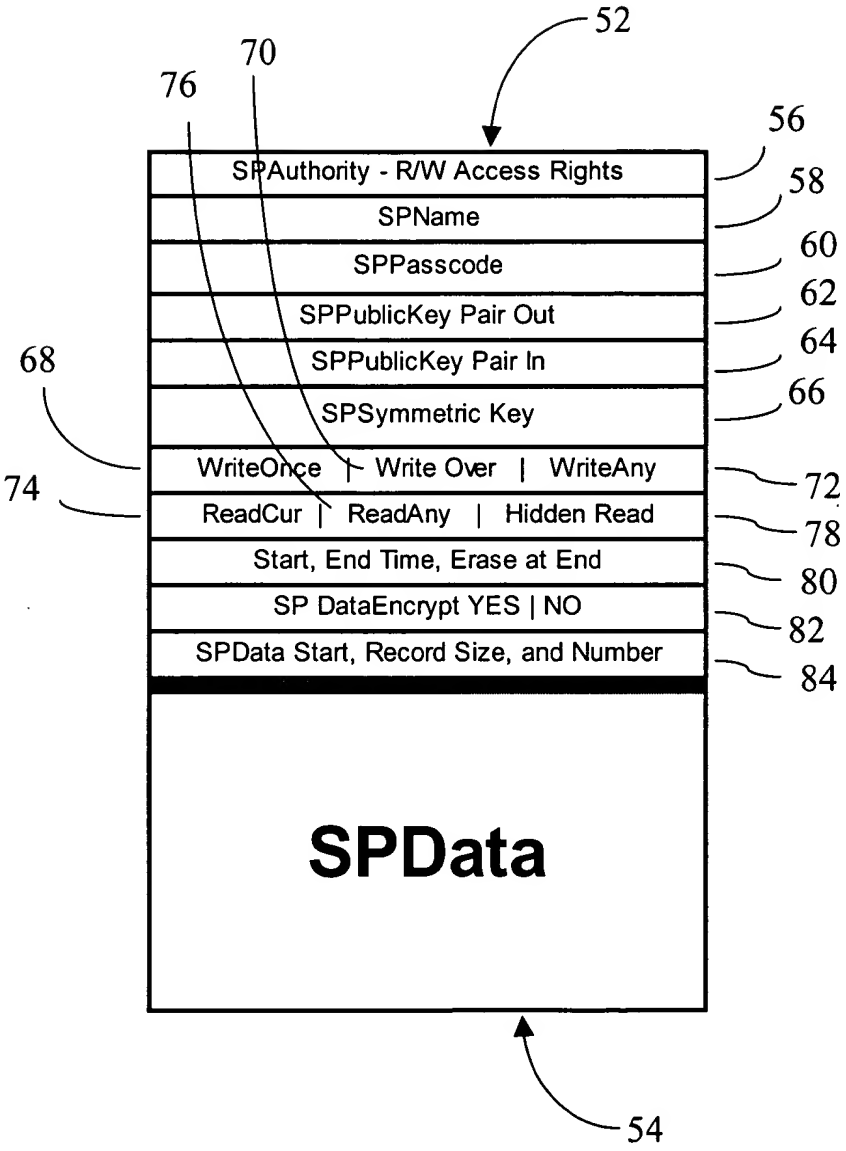
52
70
76
56
SPAuthority - R/W Access Rights
58
SPName
60
SPPasscode
62
SPPublicKey Pair Out
64
SPPublicKey Pair In
68
66
SPSymmetric Key
74
WriteOnce | Write Over | WriteAny
72
ReadCur | ReadAny | Hidden Read
78
Start, End Time, Erase at End
80
SP DataEncrypt YES | NO
82
SPData Start, Record Size, and Number
84
SPData
54

FIG. 4

FIGURE 5

					Authority Source (See AuthSet Call)		
Field	**N**	**Bit Size**	**Byte Size**	**Note**	**Internal**	**External**	**Root**
SPName	1	256	32	First Byte Null	InFrom Set	InFrom Set	InFrom Set
SPPasscode	1	128	16		InFrom CSet, Hidden	InFrom CSet, Hidden	InFrom CSet, Hidden
SPPublicKey-Out	1	4096	512		OutFrom Set	InFrom CSet, OutFrom Set	OutFrom Set
SPPrivateKey-Out	1	4096	512		Hidden	InFrom Set, Hidden	Hidden
SPPublicKey-In	1	4096	512		OutFrom Set	InFrom Cset	OutFrom Set
SPPrivateKey-In	1	4096	512		Hidden	InFrom CSet, Hidden	Hidden
SPSymKey	1	1024	128		Hidden	InFrom CSet, Hidden	Hidden
SPNonce	1	2048	256	avoid replay attacks	In | Out from Set	In | Out from Set	In | Out from Set
SPAuthSource (Internal | External | Special)	1	2	0.25		Not Applicable	Not Applicable	Not Applicable
SPDataWriteMode (WriteOnce | WriteOver | WriteAny)	1	2	0.25		InFrom Set	InFrom Set	WriteAny
SPDataReadMode (ReadCur | ReadAny | Hidden)	1	2	0.25		InFrom Set	InFrom Set	ReadAny
SPDataEncrypt (YES | NO)	1	1	0.125		InFrom Set	InFrom Set	InFrom Set
SPStartTime	1	128	16		InFrom Set	InFrom Set	InFrom Set
SPEndTime	1	128	16		InFrom Set	InFrom Set	InFrom Set
SPEraseAtExpiration (YES | NO)	1	1	0.125		InFrom Set	InFrom Set	InFrom Set
SPNumberofRecords	1	64	8		InFrom Set	InFrom Set	InFrom Set
SPRecordSize	1	64	8		InFrom Set	InFrom Set	min 3270
SPCurrentRecord	1	64	8		InFrom Set	InFrom Set	-1
SPDataStart (an absolute disk address)	1	768	96		Hidden	Hidden	Hidden
SPAuthority SPName (reader, writer, admin, encrypted passcode, certIN, certOut)*	64	32	256	First Byte Encodes REQUIRES	InFrom Set	InFrom Set	(1,1,1,1,1,1,..)
Total Bytes in One Auth Record		21,096	2,889				
Rounded Up			3,072		6 Disk Blocks		
SPData (the disk address for this is usually not contiguous with the authority record).		SPRecSize * NumRecs	193,536 is 3,072*63 for the Root Data	Other Authorities will have other Sizes			

FIGURE 6

Field	Bits	Bytes	Example	Notes	
SPMagic	32	4	xF27F		
SPOffset	32	4	1844	header size may increase by more than one disk begin-end storagelimit item	
SPVersion	32	4	1.01	text	
SPCryptoSuite	128	16	RSA+RAJD++	text	Fixed in the Preferred Embodiment
SPVendor	128	16	Foobar Corp.	text	
SPNumAuths	32	4	64		
SPAuthSize	32	4	6	In 512 Byte Blocks	
SPRootPublicKeyIn	4096	512			From Root Auth Record
SPRootNonce	2048	256			Synthesized on demand
SPStorageLimits	8192	1024		Begin/End Absolute Disk Locations	Synthesized from Auth Records

Note: Authority Partition Header is typically not writeable.

FIGURE 7

Call	Arguments					Notes	
Calls that Read and Write Authority Records							
SPAuthHeader	AuthHeader					Returns Header	
SPSet	Name	Passcode CertIN	CertOut	AuthRecord	View | Modify | Add | Delete	Sets values for an authority	requires Admin priviledge
SPCSet	Name	Passcode CertIN	CertOut	AuthRecord	View | Modify | Add | Delete	Secure Setting of values for authority, utilizes public key	requires Admin priviledge
Calls that permit conventional Read and Write of Authority Data Records							
SPOpen	Name	Passcode CertIN	CertOut	AuthRecord	Duration in Microseconds	Opens an SDpartition for authorized read and write	
SPClose	Name	Passcode CertIN	CertOut	AuthRecord		Closes an Sdpartition for authorized read and write	
Calls that utilize SP's ability to hide secrets and hide basic cryptography							
SPSignThis	Name	Passcode CertIN	CertOut	DatatoSign	PrivateKeyLocation	SignedData(returned)	
SPCheckThis	Name	Passcode CertIN	CertOut	DatatoCheck	PrivateKeyLocation	Check(returned)	
SPProtRead	Name	Passcode CertIN	CertOut	Data (returned)	MyPublicKey	Location	
SPProtWrite	Name	Passcode CertIN	CertOut	Data	MyPublicKey Location	Location	SPSuccess (returned)
SPHashThis	Name	Passcode CertIN	CertOut	DatatoHash	Hash (returned)	Location to Store	

Note.: Locations above are possibly complex in that they can specify other authority records that this authority has the right to read or write. So the location may be Name:RecordNumber, in general.

FIGURE 8

Error	Code	Notes
SPSuccess	0	
SPBad CertificateIN	1	Certificate In Failure
SPBad CertificateOUT	2	Certificate Out Failure
SPBad Name	3	Name not found
SPBad Passcode	4	Passcode failed
SPNo PublicKey-Out	5	For External Authority
SPNo Publickey-In	6	For External Authority
SPNo PrivateKey-Out	7	For External Authority
SPNo PrivateKey-In	8	For External Authority
SPNoAuthority	9	You can't do this
SPPartition Full	10	The SP Partition is Full and writeover is not turned on
SPNo Space For Partition	11	You can't create this partition, no continguous space
SPNo Security Support	12	SP Security Turned off on this device - Header Fail
SPRead Failure	13	Special SP Read Failed
SPWrite Failure	14	Special SP Write Failed